UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

Malibu Media, LLC,

Plaintiff,

vs.

John Doe,

Defendant.

CIVIL ACTION NO. 17-cv-09962-KPF

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANT'S MOTION TO IMPOSE SANCTIONS OR A CONTEMPT ORDER AND TO DISMISS THE COMPLAINT

SUMMARY STATEMENT

Defendant John Doe respectfully moves the Court for 1) an order dismissing the complaint and ordering payment from Plaintiff and Plaintiff's counsel in an amount that the Court deems appropriate as a sanction and for civil contempt and 2) an order dismissing the complaint for failure to state a claim.

Plaintiff and Plaintiff's counsel violated this Court's order that they protect Plaintiff's anonymity and they lack any mitigating evidence.

Additionally, the complaint should be dismissed for failure to join necessary parties and for failure to state a claim upon which relief can be granted. *See e.g.*, *E.g.* Matthew Sag, Jake Haskell, *Defense Against the Dark Arts of Copyright Trolling*, 103 Iowa L. Rev. 571 (2018).

FACTUAL BACKGROUND[1]

BitTorrent is a popular method of sharing digital files (the "BT Method") using the Internet. Countless types of digital files can be shared including photographs, movie files, music files, e-book files, or collections of these and any other files that can be opened on a computer (collectively "Digital Files").[2] The BT Method is popular because it reduces the time it takes to send large files between computers by breaking the large files into small pieces, and sending these small pieces to other computer where they are reassembled into the original Digital File.

The BT Method works as follows:

[1] This document was prepared with the assistance of the New York Legal Assistance Group's Legal Clinic for Pro Se Litigants in the SDNY.

[2] See https://www.makeuseof.com/tag/8-legal-uses-for-bittorrent-youd-be-surprised/ and http://www.cbc.ca/news/entertainment/cbc-tv-first-in-north-america-to-release-prime-time-show-on-bittorrent-1.749301

1. Create. Users who possess a Digital File that they want to share using the BT Method that is not currently being shared ("Uploaders")[3] must first download and install a computer program called a client ("Client"). The Client divides the Digital File into smaller pieces (the "Pieces") that are each given a unique identifying number called a piece hash ("Piece Hash"). There are a number of different computer programs that serve as "Clients".[4] Notably, the Pieces of a Digital File are not all the same file size, or do they contain equal portions of certain types of information in the Digital File.[5] For example, when a Client divides a Digital File of a home video, one Piece might contain code that the states that the movie contains images that are color vs. black and white, and also contain information that it is a file that should be opened in a program like iTunes, and not in Microsoft Word. Other Pieces may contain images or audio from the home movie.

When a Client divides a Digital File into Pieces, it also creates an instruction manual of how to put these Pieces can back together. These instructions are contained in a new file called a torrent file ("Torrent File").[6] The Torrent File is also assigned a unique identifying number, called an info hash ("Info Hash").[7] Torrent Files are significantly smaller than Digital Files, as each Torrent File only contain the instructions of how to put together a related Digital File. By way of analogy, the Torrent File is comparable to the instructions included in a Lego Set, and the actual Lego pieces in a set are comparable to the Pieces of the Digital File. Once the Uploader has created the Torrent File, his or her computer will contain

[3] Some materials call initial uploaders "Initial Seeders."
[4] See https://lifehacker.com/285489/a-beginners-guide-to-bittorrent
[5] http://www.morehawes.co.uk/the-bittorrent-protocol
[6] See https://www.makeuseof.com/tag/free-torrent-guide/
[7] See http://www.bittorrent.org/beps/bep_0003.html

both (a) the Digital File and (b) the accompanying Torrent File. The Uploader has the ability to change the name of the Digital File and the Torrent File to a name of his or her choosing. [8]

2. Upload. The Uploader may then access and upload the Torrent File to a website (an "Torrent Site") that hosts a number of different Torrent Files that are accessible and downloadable. When uploading the Torrent File to an Torrent Site, the Uploader provides the Index with a name that advertises to the Torrent File for downloading ("Downloading Name").[9] This Downloading Name can be different from the name of the original Torrent File, and also different from the name of the original Digital File. The Uploader does not upload the Digital File to the Torrent Site, nor will it ever be uploaded to the Index using the BT Method. The Torrent File will now be available for access to anyone searching that particular Torrent Site.
3. Search. Users with Internet access can search an Torrent Site for a Torrent File associated with a desired Digital File. For example, a user could search "Nimmer" to see if anyone person had uploaded a Torrent File for a digital copy of the popular copyright treatise on that particular Torrent Site. Obviously, Torrent Files may be misnamed, which can result in a user thinking that they are downloading a Torrent File that corresponds to a lecture on the copyright treatise, when they are in fact downloading a Torrent file that corresponds to a CareBears episode.
4. Share. Once the Torrent File is downloaded, the user then opens the Torrent File in a Client. When the user opens the Torrent File in the Client, the User has the option to choose whether or not to begin downloading the Digital File they believe is associated with the Torrent File. Pieces of a Digital File are sent directly from the computer of a user who wishes to download the file and has the related Torrent file ("Peers") and the computer of anyone else using a

[8] See https://lifehacker.com/5534190/how-to-share-your-own-files-using-bittorrent
[9] See Id.

Client who has (a) the Client open on their computer; (b) the original Digital File; (c) the related Torrent File; and (d) chosen to share the Digital File with other users ("Seeders") when a Peer's computer and Seeder's computer are connected. The connection between a Peer's computer and and Seeder's computer is made using an online server called a tracker ("Tracker"). Trackers monitor which Peers require a Piece of a Digital File, and the Seeders who have the required Piece on his or her computer. Peers' and Seeders' computers contact the Tracker by using an internet connections that is associated with a specific IP address. The Tracker then brokers the sharing of the Piece between Peer and Seeder. [10]

The number of Peers and Seeders downloading and sharing a Digital File via the BT Method can vary. For example, if there is only one person who has (a) a Client open on his or her computer, (b) the original Digital File, (c) the related Torrent File; and (d) chosen to share the Digital File with other Peers, then a Peer will download the entire digital file from this Seeder. If there are multiple Seeders who have (a) a Client open on his or her computer, (b) the original Digital File, (c) the related Torrent File; and (d) chosen to share the Digital File with other Peers, then the Peer's computer will identify the fastest available connection between a Peer and a Seeder, and download a Piece of the Digital File.[11]

The Peer does not need to download the Pieces of a Digital File in any particular order. The Client uses the outline contained in the Torrent File to automatically choose which Seeder to download any particular Piece from and the order in which the Pieces are downloaded. The Client also prevents the Peer from downloading any particular Piece twice. The Peer's computer establishes a connection with each Seeders' computer directly, and so none of the pieces of the original Digital File is never uploaded onto any third party server or

[10] See https://www.makeuseof.com/tag/free-torrent-guide/.
[11] See https://lifehacker.com/5310210/speed-up-your-downloads-by-choosing-the-fastest-torrents.

website. This method of downloading small pieces of an original digital file in a seemingly random order permits the Peer to download a file as long as at least one Seeder has (a) a Client open on his or her computer, (b) the original Digital File, (c) the related Torrent File; and (d) chosen to share the Digital File with other Peers.

A Peer may also be a Seeder. In other words, a person who uses a Client may permit others to establish a direct connection with his/her computer to directly download pieces of original digital files from him/her. Generally, there is an option in a Client to prohibit others from downloading a Digital File from your computer, that is, to prohibit a Peer from leeching a Digital File.[12] The Peer need not have all of the pieces for a Digital File for another Peer to download a Piece from his or her computer. In fact, if a Peer only has a single piece, other Peers may still download that piece from that Peer.[13] Since the Client can only convert the Pieces of Digital File into a usable form when the Peer has all of the pieces of a particular Digital File, a Peer can share Pieces of a Digital File with others, even though the Peer cannot use or even open the Digital File himself/herself. As a result, a Peer may seed files that he or she does not know the contents of to other Peers.

5. Complete. As Pieces are downloaded, the Client, in connection with the Torrent File, determines whether a Peer has downloaded all Pieces of a Digital File. This analysis is performed using the Hash Values of each Pieces and outline of the Digital File contained in the Torrent File. If all the Hash Values associated with a Digital File are presented, then all the Pieces of the Digital File have been downloaded. When all of the Pieces the Digital File are downloaded, the Client arranges the Pieces and assembles the Digital File in a usable form. A Peer is unable to to use or open a Digital File unless the Peer possesses all pieces of

[12] See https://techjourney.net/how-to-disable-upload-turn-off-seeding-in-utorrent/
[13] https://www.techworm.net/2017/03/seeds-peers-Peers-torrents-language.html

the the entire original Digital File.[14] Notably, Courts have held that copyright infringement only occurs complete when each of the piece hashes have been downloaded correctly and a full and complete digital file is created on the infringer's computer.

Procedural History

Plaintiff is a pornographer that photographs and films sexual acts and then distributes those sexually explicit images and recordings on the internet. Plaintiff distributes its products for free on various video sharing sites and in other forms on the internet. A person can purchase may also purchase complete unlimited access to all its films on the Plaintiff's website for a nominal monthly fee of $29.95. Join Now Page on X-Art.com, last accessed on April 27, 2018, available at:

https://bill.ccbill.com/jpost/billingCascade.cgi?clientAccnum=928532&clientSubacc=0001&cas
c
adeId=17337&ACH=0000001161:978,0000776079:978,0000000037:978,0000000138:978,0000
001161:840,0000776079:840,0000000037:840,0000000138:840&CC=0000001161:840,000077
6079:840,0000000037:840,0000000138:840&DP=0000000138:978,0000776079:978&subscripti
onTypeId=0000001161:840&sitename=x-art.com.

This Plaintiff has brought thousands of lawsuits to enforce copyrights against tens of thousands of Defendants. *E.g.* Matthew Sag, Jake Haskell, *Defense Against the Dark Arts of Copyright Trolling*, 103 Iowa L. Rev. 571, 578 (2018); *see Malibu Media, LLC v. John Does 1-10,* No. 2:12-cv-003623-OD-PJWx, 2012 WL 5382304, at *4 (C.D. Cal. June 27, 2012) ("The Court will not idly watch what is essentially an extortion scheme, for a case that plaintiff has no intention of bringing to trial."). According to a 2016 Bloomberg Law Article, "Malibu files up to 40 percent of all copyright claims in U.S. federal court… [t]he company has filed more than

[14] See https://lifehacker.com/5599680/resume-interrupted-downloads-with-bittorrent

5,000 lawsuits [from 2012 to 2016]"[15] alone. Currently, a search of the Southern District of New York's electronic filing system alone reveals 59 such open cases before multiple Judges.

On February 13, 2017, Plaintiff filed an action in this Court under docket number 1:17-cv-01078-KPF alleging a violation of copyright against a "John Doe Subscriber assigned IP Address 68.174.66.36." There was only one defendant in that case. Plaintiff then sought and was granted leave to serve a third party subpoena on an internet service provider to obtain that John Doe's name and address. However, the Court explicitly ordered that "Defendant may proceed anonymously as John Doe unless and until the Court orders otherwise." *Malibu Media, LLC v. Doe*, 1:17-cv-01078-KPF, ECF # 11 (March 17, 2017). After receiving notice from his internet service provider that it believed Defendant was that John Doe, Defendant requested and was granted leave to proceed anonymously, ECF # 21-22 (August 24, 2017). At no point, did the Court order that his identity could be revealed.

On September 13, 2017 Plaintiff made a second request for an extension of the deadline to serve the complaint, which was granted. ECF #24-25. On October 15, 2017, one day before the service deadline, Plaintiff voluntarily dismissed the case. Defendant was never served under that case number despite Plaintiff having his personal information, including name and current address.

At no point has Plaintiff provided the Court with any explanation for failing to proceed under that case number. Instead, on December 21, 2017, Plaintiff filed the instant action, 1:17-cv-09962-KPF, which is simply a re-filing of the earlier action under a separate case number. This circumvented the Court by bringing the action under Defendant's full name. This case disclosed Defendant's identity in direct violation of the Court's March 17, 2017 and August 24, 2017 orders in the previous case.

[15] https://www.bna.com/porn-infringement-battles-n57982073918/

On February 20, 2018, Defendant again requested the Court leave to proceed anonymously as well as other relief which would protect his identity. ECF #11. On February 21, 2018, Your Honor granted the request and the case was sealed and all identifying information redacted. ECF #12.

On March 9, 2018 the Court held a conference in this case. At that conference, Plaintiff's counsel stated that the filing of the case using Defendant's name was an "accident." Plaintiff's counsel stated that ordinarily, the Plaintiff files a single case against many John Doe Defendants, and then brings new separate actions against the individual defendants. Plaintiff's counsel provided no explanation for how this "ordinary" procedure led to the "accident" in this specific matter, which was originally brought against a single defendant, not several.

The Underlying Allegations of the Case

The Court is familiar with the Plaintiff's allegations, and Plaintiff need not recite them here. However, Plaintiff writes to highlight certain portions of Plaintiff's allegations.

First, Plaintiff makes no allegation that Defendant was the first person to share the movies at issue in this case as an Initial Uploader or Seeder.

Second, Plaintiff only makes a conclusory allegation that Defendant possessed a complete copy of the entire Digital File. *Comp.* ¶ 23. Plaintiff provides no basis for this factual claim or source of information.

Third, from Plaintiff's pleading, there is no indication that Defendant had any knowledge that the files infringed on Plaintiff's copyright. Assuming that Plaintiff's investigators used standard BitTorrent procedure to establish the direct connection, Plaintiff does not indicate the "name of" of the Torrent Files on the relevant Index or in the relevant client. In other words,

Plaintiff does not provide any indication that any of the file names at issue in this case would have alerted a "Peer" that the copyright to the individual digital files were not owned by the original uploader (aka initial seeder) or part of the public domain. In fact, Plaintiff fails to provide any indication that the file names were accurate, nongeneric, and infringing. As pled, the names of the files could have been inaccurate, such as "magna carta." Or the names could have been generic, such as a simple description of the movies' content. Even the titles used by Plaintiff in the pleadings to identify the original movies are generic descriptions of the movies' content. There is no indication that "X-Art," the underlying copyright owner, was identified in the file name.

Along these same lines, while Plaintiff fails to allege that Defendant viewed the movies or had any knowledge of their content, Plaintiff fails to indicate that the movies allegedly shared by Defendant (or even the original movies as created by Plaintiff), provided any notice that the film was protected by copyright. There is no allegation that the original movie, or the version allegedly shared, contained an FBI Seal, credits, or a logo.

Fourth, Plaintiff doesn't describe how it's investigators established a "direct TCP/IP connection" with the IP address stated in the complaint. The investigators do not state if they used traditional BitTorrent technology to establish that connection. In BitTorrent terms, they do not state if the investigators acted as Peers and someone using the IP address acted as a Seeder.[16] *See Complaint* ¶ 17. Accordingly, Plaintiff does not indicate how its investigators identified the IP address as the source of any of the BitTorrent pieces that Plaintiff's investigators used to create a complete digital media file. *See Complaint* ¶ 18. In fact, the complaint doesn't even identify the hash value for any of the individual pieces that Plaintiff's investigators traced to the

16

IP address in the complaint. The complaint only identifies the hash value for the complete digital file. *See Complaint* ¶ 19, 20.

Nor does the complaint address any of its efforts to counteract "IP spoofing" which is when one user pretends to have the IP address of another.[17] This practice allows bad actors to "steal" an IP address associated with another computer, download files using this IP address to the bad actor's computer, and and then return the stolen IP address.[18] Doing so effectively protects bad actors from using their IP addresses to engage in nefarious activity and implicates. Furthermore, some Clients and Indices have been found to install malware and other nefarious programs onto a Peer's computer that can allow for this or similar practices. [19]

Argument

As Defendant is Pro Se, Defendant asks the Court to consider Defendant's briefing papers liberally to raise the strongest arguments they suggest. *McLeod v. Jewish Guild for the Blind*, 864 F.3d 154, 156 (2d Cir. 2017). While Plaintiff has received assistance from the New York Legal Assistance Group's Legal Clinic for Pro Se Litigants in the Southern District of New York, the Clinic's limited assistance is no substitute for the full representation of counsel.

I. THIS COURT SHOULD SANCTION, OR HOLD IN CONTEMPT, PLAINTIFF AND PLAINTIFF'S COUNSEL FOR DISOBEYING THIS COURT'S ORDER THAT DEFENDANT REMAIN ANONYMOUS AFTER ALREADY HAVING RECEIVED OPPORTUNITIES TO CORRECT THEIR BEHAVIOR IN OTHER CASES

---

[17] https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

[18] https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-38/104-ip-spoofing.html

[19] See http://www.digitalcitizensalliance.org/news/press-releases-2015/digital-bait-internet-users-at-high-risk-of-malware-from-content-theft-70-million-underground-market/; see also https://lifehacker.com/torrenting-showdown-transmission-vs-qbitorrent-vs-tor-1786122054 ; see also https://www.theinquirer.net/inquirer/news/2471692/hackers-are-spiking-torrent-downloads-with-malware

Plaintiff has been cited by numerous Courts across multiple jurisdictions for engaging in inappropriate conduct. For example, Judge Hellerstein noted in one opinion that "Malibu's corporate strategy relies on aggressively suing for infringement and obtaining accelerated discovery of the IP address holder's identity from the ISP. It then seeks quick, out-of-court settlements which, because they are hidden, raise serious questions about misuse of court procedure. Judges regularly complain about Malibu." *Malibu Media, LLC v. Doe,* 2015 WL 4092417, at *4 (S.D.N.Y. 2015). "Malibu effectuates its strategy by employing tactics clearly calculated to embarrass defendants." *Id.,* at *3.

Previous admonishments have not slowed down Malibu Media and it has continued to use questionable methods in their myriad of copyright litigation across the country. Previously, while their conduct may have skirted the edges of permissible litigation methods, in the instant case, their tactics have blatantly crossed the lines of appropriate conduct.

"A court of the United States shall have power to punish by fine or imprisonment, or both, at its discretion, such contempt of its authority, and none other, as . . . [d]isobedience or resistance to its lawful writ, process, order, rule, decree, or command." *18 USCA § 401* (3) . "[I]n order to hold the alleged contemnor in contempt, the court need only (1) have entered a clear and unambiguous order, (2) find it established by clear and convincing evidence that the order was not complied with, and (3) find that the alleged contemnor has not clearly established [her] inability to comply with the terms of the order." *Corporation v. Rice, 2016 WL 397673,* at *2 (SDNY 2016).

First, there was a clear and unambiguous order that Defendant remain anonymous in this litigation. Second, there is clear and convincing evidence that Plaintiff and Plaintiff's counsel did not comply with the Court's order in the form of court filings revealing Defendant's identity.

Third, Plaintiff and Plaintiff's counsel have failed to establish inability to comply with the terms of that order. Here, Plaintiff could have served Defendant under the earlier docket where Defendant was already anonymous. Instead, Plaintiff chose to withdraw the case and file the instant action. Plaintiff has provided no explanation for not proceeding in the earlier case. Additionally, even if Plaintiff had adequate justification for failing to meet the service deadline in the previous action and decided instead to withdraw and file under a new docket, Plaintiff has provided no reason for not complying with the Court's earlier orders by identifying the Defendant as a John Doe. Nor has Plaintiff claimed to have attempted to comply with that order.

At the conference on March 9, 2018, Plaintiff's counsel stated that it was standard practice to break up an original case against a group of Does into separate cases against named individuals when the identities of the Does were revealed. This was an odd explanation from Plaintiff's counsel. To begin with, this standard practice comports with the frequent allegation that Plaintiff, Malibu Media, and it's counsel use the judicial system to extort money by making embarrassing allegations. Additionally, the earlier case where Your Honor ordered Defendant's anonymity was not a case against "a group of Does." The case was filed against only one Defendant with his IP address as identifier. So that explanation has no bearing on this case. Even if that explanation did have bearing, it would not excuse the failure to comply with the Court's order.

Plaintiff and Plaintiff's counsel had two opportunities to provide an adequate explanation to the Court for their disregard of the Court's earlier order, and failed twice. At that conference, opposing counsel was already on notice that Defendant would be seeking sanctions for revelation of his identity because Defendant had filed a request for a pre-motion conference prior to the conference. ECF # 18 (March 6, 2018). Additionally, in an earlier letter to the Court, opposing

counsel stated that the "initial naming of Defendant in this matter was inadvertent." ECF # 19 (March 8, 2018). The Court should reject any new attempts at explaining the behavior of Plaintiff and Plaintiff's counsel.

Furthermore, despite the Court's granting his request to seal the current case and redact any identifying information that would put Defendant at risk of false identification, Plaintiff's unlawful actions have already irreparably harmed Defendant. A simple online search reveals at least four instances of published information from this case including the full text of the Complaint's allegations.[20] Defendant does not know how much time, effort, and resources he will need to allocate to remove these public pages controlled by private third parties, or if he could ever be successful. By directly disobeying the Court's orders, Plaintiff and Plaintiff's counsel have put the Defendant's reputation in jeopardy and put him in constant risk of being rejected by an employer searching the internet. Moreover, the Defendant has received at least four different solicitations by mail from law firms offering their services in defending this lawsuit. It is obvious that in the short time his full name was published online as a Defendant in this action, it has been flagged and submitted to at least one publicly available database with his personal contact information. Defendant does not know how many databases his personal contact information was submitted and he is fearful that his name and contact information will forever be associated as a Defendant in pornography copyright infringement litigation.

Plaintiff, Malibu Media, has a voluminous history of inappropriate conduct. *Malibu Media, LLC v. Doe*, 2015 WL 4092417, at *4 (S.D.N.Y. 2015) (refusing to issue a subpoena for the identity of an internet user). Given Plaintiff's limited resources, he has been unable to fully comb through the mountains of legal writing condemning their behavior. *Id.* While Plaintiff is

[20] To continue to protect Defendant's identity, Defendant has left the URL's of those websites off this memorandum of law. However, Defendant can provide a list of these sites to the Court and opposing counsel upon request.

certain that other examples exist, he has identified at least two other occasions of Plaintiff violating court orders concerning a Defendant's identity.

In *Malibu Media, LLC v. Doe,* No. 1:14–cv–493, 2015 WL 3417432, at *4 (S.D.Ohio 2015) extremely similar to here, the Court issued two unambiguous orders that Malibu Media file the Defendant's name under seal, but Malibu Media filed it publicly. In that case, Malibu Media's counsel erroneously believed that it was possible to file documents under seal electronically instead of in person. *Id.* Although Malibu Media's counsel attempted to make that filing under seal, the filing was public despite counsel's attempts. Additionally, in that case, Defendant's identity was only public for approximately 15 hours, Defendant did not allege that anyone actually learned his identity, or that he suffered any actual loss. In light of counsel's attempts to file under seal and the lack of allegations of harm to Defendant, the Court chose not to impose sanctions, and actually modified its document filing process. *Id.* Approximately two weeks after that decision, Malibu Media voluntarily dismissed the case.

In contrast, here Plaintiff's counsel made no attempt to file the documents anonymously or under seal. In fact, here, Plaintiff's counsel took additional steps to file the suit publicly, including paying an additional filing fee. Moreover, Defendant has alleged that he suffered harm because his information was available for longer than 15 hours, approximately two months on the Court's website, and perhaps forever on the internet. Here, Defendant has also adequately shown that others have learned his identity in association with this case. Defendant now faces a continuous harm from Plaintiff's complete lack of attempt to protect his identity. In the Southern District of Ohio case, the Court trusted that Malibu Media and it's outside counsel Lipscomb, Eisenberg & Baker "had received the message." Malibu's actions in this case reveal that Judge

Black's trust was misplaced. While Plaintiff's misconduct is voluminous in other cases, this case alone demonstrates the need for sanctions or contempt findings.

In *Patrick Collins, Inc. v. Doe 1*, 2:12-cv-01154-ADS-GRB, 288 F.R.D. 233, 236 (E.D.N.Y. Nov. 20, 2012), the Court explicitly ordered that the information containing Defendant's identity be sent from the subpoenaed directly to the Court, "ex parte and under seal." Instead, Malibu Media served subpoenas that requested the identifying information be sent directly to Plaintiff's counsel, in direct violation of the Court's order. That case was eventually dismissed pursuant to stipulation. *Id.* at ECF # 40 (July 19, 2013).

In light of Plaintiff's history of disobedience, Judge Hellerstein denied Malibu Media's attempts to even serve a subpoena on an internet service provider. Judge Hellerstein also noted that "[w]hen courts have attempted to place restrictions on the subpoena to prevent Malibu from abusing the process to extort defendants, Malibu has flagrantly disregarded them." This case here, is a textbook example of Malibu Media's disregard of attempts by the judiciary to place limits on its ability to extort defendants.

Having filed thousands of similar actions in district courts across the country, Plaintiff Malibu Media is a sophisticated and experienced litigant represented by counsel, and such cynical disregard to Court orders should be duly sanctioned or held in contempt. "[I]t is well established that "courts have inherent power to enforce compliance with their lawful orders through civil contempt." *Gucci America, Inc. v. Li,* 2015 WL 7758872, at *1 (SDNY 2015). "[I]mposition of civil contempt sanctions may serve dual purposes: to secure future compliance with court orders and to compensate the party that has been wronged." *Philip Morris USA Inc. v. Los Corazones Deli Grocery Inc.,* 2014 WL 4363836, at *2 (SDNY 2014).

Accordingly, Defendant respectfully requests the Court issue sanctions and findings of contempt against both Malibu Media and counsel Kevin T. Conway, including but not limited to dismissing Plaintiff's claims in their entirety, appropriate monetary compensation, and for such other further relief that the Court deems just and proper.

II. THIS COURT SHOULD DISMISS THE COMPLAINT

a. Plaintiff Failed to Join Indispensable Parties Under FRCP Rule 19

Here, failure to join the initial uploader or allege that Defendant is the initial uploader requires dismissal of the case.

Failing to join the initial seeder would subject the Defendant to incurring an inconsistent obligation and otherwise impede his ability to protect his interests. "A person who is subject to service of process and whose joinder will not deprive the court of subject-matter jurisdiction must be joined as a party if: …(B) that person claims an interest relating to the subject of the action and is so situated that disposing of the action in the person's absence may: (i) as a practical matter impair or impede the person's ability to protect the interest; or (ii) leave an existing party subject to a substantial risk of incurring double, multiple, or otherwise inconsistent obligations because of the interest." see *Fed R. Civ. Pr., Rule 19. Required Joinder of Parties.*

Plaintiff asserts that "[i]n order to distribute a large file, the BitTorrent protocol breaks a file into many small pieces. Users then exchange these small pieces among each other instead of attempting to distribute a much larger digital file." Complaint ¶12. Plaintiff fails to include any allegations against the initial seeder or other alleged participants. Under Plaintiff's own proposed infringement theory, the alleged infringement is impossible without at least an initial seeder and multiple additional subsequent participants, who may very well have had a legal privilege to

publish or distribute the works for free. In the context of peer to peer theory, any action against an alleged file sharer requires at a minimum the joinder of the initial seeder.

Indeed, as per Plaintiff's own proffered exhibits, the alleged infringement occurred soon after the movies were published. So soon in fact, that Plaintiff did not even register the works prior to the alleged infringing activity or the ensuing "investigation" to uncover such infringement. As such, it is highly probable that the initial seeder, having such early access to the file in question, was in fact someone with a legal right to distribute the films for free. Going through the list of alleged infringing activity, there appears to be an obvious pattern of publishing, ensuing investigation to uncover infringers, and registration of a copyright only after the alleged infringement was claimed to be observed.

Not only is this action a classic example of copyright trolling, Plaintiff's prolific litigation over the past few years has been categorized as such by judges across the nation. *See e.g. Malibu Media, LLC v. Doe,* 2015 WL 4092417, at *2 (S.D.N.Y.,2015) *quoting Matthew Sag, Copyright Trolling, An Empirical Study,* 100 Iowa L.Rev. 1105, 1108 (2015) ("Recent empirical studies show that the field of copyright litigation is increasingly being overtaken by copyright trolls, roughly defined as plaintiffs who are more focused on the business of litigation than on selling a product or service or licensing their [copyrights] to third parties to sell a product or service.") *(internal quotations omitted)*

b. The Complaint Fails to State a Claim Under FRCP 12(b)(6)

"To survive motion to dismiss, complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face; claim has "facial plausibility" when plaintiff pleads factual content that allows court to draw reasonable inference that defendant is liable for misconduct alleged." *Ashcroft v. Iqbal, 556 U.S. 662 (U.S.,2009).* Even if all of

Plaintiff's facts are accepted as true, the complaint cannot survive a motion to dismiss because Plaintiff fails to plead sufficient factual content which would allow the court to draw a reasonable inference that Defendant is liable for the copyright infringement alleged.

i. Plaintiff Did Not Sufficiently Plead a Prima Facie Case of Copyright Infringement Because Plaintiff did not Show that Plaintiff's Investigation was Reliable, Valid, or Proper

Plaintiff attempts to use elaborate explanations and offers what at first glance may seem like facts giving credibility to their "investigation" process, however, upon closer look, their entire complaint and "facts" are nothing more than a cookie cutter statement, made up of smoke and mirrors, half-truths and rhetoric. Plaintiff files thousands of these complaints knowing that a large percentage of the defendants will settle, fearing the association of their name with such a questionable subject matter – with no intention of going to trial.

Plaintiff admits to using IPP International, (IPP), as its "investigator" and claims that "[b]ased upon experience filing over 1,000 cases the geolocation technology used by Plaintiff has proven to be accurate to the District level in over 99% of the cases." However, the complaint fails to mention how many of these cases if any were actually adjudicated on the merits. In fact, after researching the issue, Defendant was unable to find a single case adjudicated on the merits in Plaintiff's favor when Defendants did not concede downloading the Plaintiff's movies in violation of copyright. *See* Matthew Sag, Jake Haskell, *Defense Against the Dark Arts of Copyright Trolling*, 103 Iowa L. Rev. 571, 635 (2018) ("The plaintiffs were not put to proof in any of these cases.")

Plaintiff offers up the accuracy of their geolocation technology, yet makes no mention as to the validity of whatever software they used to track the alleged downloading of the "complete

copy of Plaintiff's works". Plaintiff does not explain the technology behind their investigation. Plaintiff does not show *how* IPP properly obtained valid, reliable data demonstrating that Defendant's IP address downloaded, shared or distributed any pieces of any copyrighted file, let alone entire files.

Moreover, Plaintiff has not explained how IPP's technology "established a direct TCP/IP connection with the Defendant's IP address." Complaint ¶ 17. It does not state if the direct connection was done by illegally hacking into some system or otherwise. Nor does the complaint state the accuracy of this data and what protections from errors, hacking, IP spoofing and other data corruption were implemented to ensure accurate and lawful data collection.

Plaintiff may not state the very facts its claims rely on in a conclusory fashion. In order to state a valid claim, Plaintiff must explain the technology behind their investigation and demonstrate the reliability of this technology and its data. As such, if the current Complaint is not dismissed outright, Plaintiffs should be required to amend their Complaint to demonstrate how their technology accurately and reliably gathers sufficient data to satisfy *Iqbal*.

ii. Plaintiff Did Not Sufficiently Plead a Prima Facie Case of Copyright Infringement Because Plaintiff did not Show that Defendant was the Alleged Infringer

"A prima facie copyright infringement claim consists of two elements: (1) ownership of a valid copyright, and (2) copying of constituent elements of the work that are original. *See Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., Inc.* 499 U.S. 3400, 361 (1991). As Judge Marrero observed in *Next Phase Distribution, Inc. v. John Does 1–27,* 284 F.R.D. 165, 171 (S.D.N.Y .2012), "if the Motion Picture is considered obscene, it may not be eligible for copyright protection." Further, even if Malibu's copyrights are valid, Malibu has not established a violation by the individual to whom the relevant IP address is registered.

In one case, Judge Oetken's opinion clearly and fully sets forth how finding an infringing IP address does not demonstrate that the owner of that IP address was the actual infringer and that cases involving pornographic materials are prone to abusive litigation tactics and coercive settlements:

> The fact that a copyrighted work was illegally downloaded from a certain IP address does not necessarily mean that the owner of that IP address was the infringer. *See e.g., In re BitTorrent Adult Film Copyright Infringement Cases,* 2012 WL 1570765, at *3 ("[T]he assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time."). Indeed, the true infringer could just as easily be a third party who had access to the internet connection, such as a son or daughter, houseguest, neighbor, or customer of a business offering internet connection. There is real risk that defendants might be falsely identified and forced to defend themselves against unwarranted allegations. In such cases, there is a risk not only of public embarrassment for the misidentified subscriber, but also that the innocent subscriber may be coerced into an unjust settlement with the plaintiff to prevent the public filing of unfounded allegations. The risk of a shake-down is compounded when the claims involve allegations that a defendant downloaded and distributed sexually explicit material.
>
> *Patrick Collins, Inc. v. Does 1-6,* 2012 WL 2001957, at *1 (S.D.N.Y. 2012)

In another opinion by Judge Spratt, the Court adopted Magistrate Judge Brown's report and recommendation that "an IP address only points to the internet account in question, and "[a]s a result, a single IP address usually supports multiple computer devices—which unlike traditional telephones can be operated simultaneously by different individuals." *Patrick Collins, Inc. v. Doe 1*, 288 F.R.D. 233, 237 (E.D.N.Y. 2012); citing *K-Beech, Inc. v. John Does* 1-37, CV 11-3995, 296 F.R.D. 80, 82 (E.D.N.Y.), report and recommendation adopted sub nom. Patrick Collins, Inc. v. Doe 1, 288 F.R.D. 233 (E.D.N.Y. 2012). "Due to the prevalence of wireless routers, the actual device that performed the allegedly infringing activity could have been owned by a relative or guest of the account owner, or even an interloper without the

knowledge of the owner." *Id.* And, "[i]f the Court were to hold internet account holders responsible for any interlopers and guests who might infringe on the Plaintiff's work, the Court would essentially be imposing a duty that every home internet user vigilantly guard their wireless network. The Court declines to impose such a duty. *See AF Holdings, LLC v. Doe,* No. 12–CV–2049, 2012 W L 3835102, at *3 (N.D.Cal. Sep. 5, 2012) ("AF Holdings has not articulated any basis for imposing on Hatfield a legal duty to prevent the infringement of AF Holdings' copyrighted works [by securing his wireless network], and the court is aware of none.")." *See Patrick Collins, Inc. v. Doe 1, 288 F.R.D. 233, (E.D.N.Y.,2012) supra at 237, 238*

Plaintiff claims that someone using Defendant's IP address infringed upon Plaintiff's copyright. Plaintiff does not state in the Complaint any facts showing that even if someone violated their copyright using Defendant's IP address, that the alleged infringer was indeed the named Defendant. Moreover, Defendant cannot be held to have held a duty to safeguard his internet connection in such a way as to prevent any attempted copyright infringement by third parties.

iii. Plaintiff Did Not Sufficiently Plead a Prima Facie Case of Copyright Infringement Because Plaintiff Did Not Show Defendant Copied, Distributed or Shared a Complete Copyrighted Work

Plaintiff attempts to explain the technical process of how a single movie file is downloaded and distributed among multiple BT users. "In order to distribute a large file, the BitTorrent protocol breaks a file into many small pieces. Users then exchange these small pieces among each other instead of attempting to distribute a much larger digital file. After the infringer receives all of the pieces of a digital media file, the infringer's BitTorrent client software reassembles the pieces so that the file may be opened and utilized…[e]ach piece of a

BitTorrent file is assigned a unique cryptographic hash value." Complaint ¶ 13-15. In their explanation, they describe two types of file types, "piece hash", representing the individual pieces of the complete files, and "file hash", representing the complete files. Here too, Plaintiff fails to offer any facts alleging that the claimed downloaded piece hashes were in fact accurately collected, observed or downloaded. Nor do Plaintiffs explain how their investigation methods could accurately hack into and manipulate a third-party software and network not developed by them or under their control without corrupting any of the hash data in the process. Fact is, that changing one tiny bit of file value, even a mere 3 characters in a 1438 character document for example, changes the hash value entirely. *See Defense Against the Dark Arts of Copyright Trolling, supra at* 594 ("[T]he 128-bit hash for the Gettysburg Address changes entirely if we change only the fourth last word from "perish" to "vanish"…[A]bout 600,000 packets of data are required to download an average film using BitTorrent."). Even if just one of these smaller piece hash values is incorrectly transmitted, logged or collected in Plaintiff's "investigation" process, the resulting full file hash will not accurately reflect the correct file information. This begs the question, how many of the tens of thousands of John Does that were named as defendants in Malibu Media's slew of copyright litigation actually downloaded or shared any of Plaintiff's registered works. Indeed, it is no wonder that Plaintiff bases his litigation strategy on getting quick pre-discovery settlements by threatening the good reputation of innocent defendants frightened by the prospect of their good name being associated with illegal pornographic downloading.

Plaintiff further alleges that "Plaintiff's investigators downloaded from Defendant one or more pieces of each of the digital media files identified by the file hashes listed. Complaint ¶18. And that "[e]ach digital media file as identified by the file hash listed…correlates to a

copyrighted film owned by Plaintiff…" and "confirmed through independent calculation that the file hash correlating to each file matched". Complaint ¶ 19- 20. However, Plaintiff again fails to allege the method or accuracy of its "findings" or how many of these file "pieces" were downloaded or distributed by Defendant. Nor does the complaint state how those alleged downloaded "pieces" constituted infringing a *completed* work sufficient to allege copyright infringement. (*emphasis added*) Another "fact" offered in this cookie cutter Complaint states "Defendant downloaded, copied, and distributed a complete copy of Plaintiff's works without authorization as enumerated on Exhibits A and B." Complaint ¶ 24. Yet, Plaintiff fails to offer any fact or evidence demonstrating that Defendant downloaded any one complete work at all. In fact, Defendant simply makes the previous statement in their Complaint as proof to their circular logic. While Plaintiffs state that their investigators observed Defendant's IP downloaded one or more pieces, Plaintiff fails to claim that Defendant's IP was observed to download or share even one completed movie file from their alleged list.

In another unsubstantiated statement, Plaintiff states that: "[a] full copy of each digital media file was downloaded from the BitTorrent file distribution network, and it was confirmed through independent calculation that the file hash correlating to each file matched… *At no point was Plaintiff's copyrighted content uploaded to any other BitTorrent user*." (emphasis added) Complaint ¶ 21. Here, Plaintiffs do not state *who* downloaded this full copy or how this independent calculation was "confirmed". (emphasis added) Curiously, Plaintiffs also claim that the copyrighted content was not uploaded to any other user – essentially stating that the file was not shared. This, despite their previous statement claiming that "Defendant downloaded, copied, and *distributed* a complete copy of Plaintiff's works without authorization as enumerated on Exhibits A and B." Complaint ¶ 24. (emphasis added).

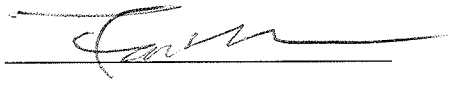
Because Plaintiff does not claim to have observed Defendant copying a completed copyrighted work, their claim for copyright infringement is invalid. *See Malibu Media, LLC v. Doe,* 2015 WL 4092417, at *5 (S.D.N.Y. 2015) *quoting Malibu Media, LLC v. John Does 1–10,* No. 12–cv–3623, 2012 WL 5382304, at *3 (C.D. Cal. June 27, 2012) ("[i]ndividual BitTorrent file pieces are worthless ... If it is the case that a Doe Defendant logged onto the BitTorrent swarm, downloaded and then uploaded a single piece to the IPP server, and then logged off, all he has done is transmit an unusable fragment of the copyrighted work....[T]he Court notes that Malibu's case is weak if all it can prove is that the Doe Defendants transmitted only part of all the BitTorrent pieces of the copyrighted work.").

It is obvious from the face of the Complaint as well as the Plaintiff's blatant disregard to this Court's Order, that the entire claim of copyright infringement is simply another attempt, out of thousands by this same Plaintiff, to blindly throw darts at some random target, hoping to achieve a quick settlement on a meritless claim. Moreover, Plaintiff is a repeat abuser of the legal system it uses to perpetuate such unethical conduct. In fact, Plaintiff does not offer any facts showing that the Defendant himself downloaded any bits of copyrighted files, let alone an entire copyrighted work, nor does Plaintiff offer facts showing that Defendant downloaded, copied and distributed such work.

As such, Defendant respectfully requests the Court dismiss the Complaint and issue sanctions or a contempt order against the Plaintiff and its counsel.

Dated: New York, New York
April 30, 2018

Respectfully Submitted,



John Doe, Defendant *Pro Se*

JOHN DOE
123 Henry St. #19
New York, NY 10002

PRO SE INTAKE UNIT
ROOM 200
500 PEARL STREET
New York, NY 10007

Re: 17-CV-9962 (KPF)

APRIL 30, 2018